Advanced Journal of Graduate Research
ISSN:2456-7108
Volume 6, Issue 1, pp. 31-40, July 2019
DOI: https://doi.org/10.21467/ajgr.6.1.31-40

GRADUATE RESEARCH ARTICLE

Relevance Feedback Utilizing Secure Evaluation with Content-based Image Retrieval in Cloud Computing

Sonali S. Panchal*, Shital Y. Gaikwad

Department of Computer Science and Engineering, Matoshri Pratishthan Group of Institutions, Institute of Engineering and Technology, SRTMUN, Nanded.

*Corresponding Author email: sonalipanchal89@gmail.com

Article History

Received: 01 March 2019
Revised: 02 May 2019
Accepted: 26 May 2019
Published: 27 May 2019

Student(s)

- Sonali S. Panchal

Academic Year: 2018-19
Course Level: Master
Course Name: Master of Engineering (M.E. Computer Science and Engineering)
Course year: 2nd year

Mentor(s)

- Shital Y. Gaikwad

ABSTRACT

Content-based image retrieval (CBIR) is the integrated system of the photograph fetching trouble for instance difficulty of chasing down pictures on a cloud in big datasets. To recognize request semantics and client's needs if you want to grant submitted consequences with reference to exactness, relevance feedback is combined into CBIR shape. Important evaluation shape will manufacture the precision of yield and will pass at hugest yield. In the watermark-primarily based tradition, a singular watermark is explicitly inserted in blended photos by means of the cloud environment earlier than photos, transmitted towards inquiry mortal. In this way, when an illicit photograph reproduction is located, the illicit inquiry mortal, where appropriates can trail the pictures with the aid of the watermark extraction. Characteristics vectors get assured by using the secure hashing algorithm, analyzing and making ready age are used at image user's aspect for confirmation motive. TPA (third party auditor) is used to understand enforcement or malevolent activities achieved in cloud circumstances. In our proposed framework, we are including the approach of misrepresentation recognition by generating trapdoor using a hashing calculation, as a document is made with the unique identifier and the client pictures with the names after the link are simplest, a trapdoor is generated.

Keywords: Content-based Image retrieval, Relevance Feedback, trapdoor generation, watermark embedding and extraction, encryption-decryption, and cloud computing.

1 Introduction

An image merits countless! That is the reason individuals as well as media, references books, and the web used pictures and designs to portray occasions, individuals, objects, circumstances. Pictures and designs are around the essential channel position for personal correspondence as they offer an upscale life of knowledge for people to understand the planet. The computerized images are the product of images components and pixels which is most usually used to suggest the additives of an advanced picture. Photo process could be a technique to remodel a picture into to transform a picture into virtual form and do some operations on that, to be able to get a bigger picture or to extract some helpful records from it. Picture seek could be specialised information explore for photos, might to boot offer question terms together with a

keyword, exposure file/tie-up or click on some photos, and also the system can return pictures "comparable" to the question. The resemblance used for seeking measures might be similar data, color allocation in photos, location/form features and so forth. Set of descriptors are furnished by means of description trendy of multimedia content material that is MPEG-7, which might be used for multimedia records description [1]. As explained in paper [1], the following are the MPEG-7 descriptors used:

- Scalable Color Descriptor (SCD): is outlined within the hue-saturation-value (HSV) color area. SCD uses a Haar work coding that permits the expandability for the characteristic extraction [1].
- Color Structure Descriptor (CSD): aims to spot the localized color allocation employing a tiny structuring window. Hue-min-max-difference (HMMD) color area is employed for the development of a color bar chart [1].
- Color Layout Descriptor (CLD): offers knowledge regarding the dimensional shading conveyance inside pictures. After a picture is partitioned into 64 squares, CLD is separated from all of those squares passionate about the separate trigonometric function amendment [1].
- Edge Histogram Descriptor (EHD): catches the structural dispersion of edges. The motion of edges may be a good surface mark for the image coordinating nonetheless once the fundamental surface isn't homogenized [1].

2 Literature Review

A picture regains system may be an automatic data processing system for browsing, looking out and recovering pictures from outsized information of digital images that utilize some technique of adding information like such as description or keywords to the pictures so that recovery of images is performed over annotation words [2]. Content-based image retrieval is additionally called query by image content (QBIC) which implies the search can establish the particular contents of an image instead of the information like tags, keywords, and/or descriptions related to the image [3]. The most focus of CBIR is low-level feature extraction that is completed from an entire image or explicit region from a picture. The most important aim of CBIR is to build techniques that may increase the retrieval accuracy and reduce regaining time [3]. The basic plan behind relevancy feedback is to integrate human interaction subjectively into the question and involve the user to assess the retrieval results. Then relying upon the user's integration, the similarity measures are mechanically refined [4]. Users will show the image retrieval system whether or not the retrieved results are "relevant", "irrelevant" or "neutral". Recovery results are then being cleared constantly. In our proposed system we are using ranking feedback type with the help of which, the user examines a set of results at a time and "sorts" them within the order she/he thinks they ought to seem. Machine learning algorithms are widely utilized in each short-term and long-term learning [2]. We are using long-term learning in our proposed system, this helps to research the link between current and past retrieval sessions mistreatment interaction or research history to model user interest [2].

Watermarking is the method that adds extra information regarding the host signal into that image itself [5]. Watermarking boost ups the safety of an inspiring image and also the ensuing image is a lot of secured, licensed and copyright protected [5]. Watermark embedding could be a method that embeds an emblem or mark image into the host image. Extraction is that method that permits the owner to be known and provides information to the meant recipients [5]. Trapdoor generation is that rule which takes the secret key as input and query picture and returns the query trapdoor TD. The secret key which is generated at the time of index generation, that key is used as query TD. So as to retrieve the much alike image, the licensed image query, the user builds, trapdoor generation to get a question trapdoor TD, and so submits the trapdoor TD, UID (User Identities) and validated key to the cloud server [1]. Trapdoor shouldn't disclose the data concerning the query picture but are usually used to search similar footage on I index. The hashing algorithm is used only for auditing and indexing of the image. In auditing fraud detection and editing is being held or not is checked. The encryption algorithm is only used to cipher plain text into encrypted text. On another side, if encrypted is being tried to edit or make deletion changes in the ciphertext, after

decryption the text will be incomplete or rather incorrect and the message couldn't be understood, for that case hashing algorithm will work by detecting fraud and making users alert.

Zhihua Xia *et al.* [1] focused on CBIR with preserving privacy and copy deterrence in Cloud Computing. For privacy-preserving purposes, sensitive images, need to be encrypted before outsourcing which makes the CBIR technologies in plaintext domain to be unusable [1]. Jing Xin and Jesse S. Jin, both in their paper titled "Relevance Feedback for Content-Based Image Retrieval using Bayesian Network" [2] focused on RF is how to effectively utilize the feedback information to upgrade retrieval presentation. This paper presents a relevance feedback scheme using a Bayesian network model for feedback information adoption [2]. Ja-Hwung Su *et al.* [6] projected a way in 2011 to realize the high potency and effectiveness of CBIR in handling the large-scale picture details. Regarding potency, the iterations of feedback are reduced well by using the navigation designs founded from the consumers query record. Related to effectiveness, the projected search algorithmic program NPRF Search makes use of the discovered navigation patterns and three sorts of question refinement methods, Question Point Movement (QPM), Query Reassigning (QR), and Query Extension (QEX), to converge the search area so as to approach the consumer's objective impressively. By applying the NPRF methodology, top quality of image recovery on RF may be gained in an exceedingly little range of feedbacks. The prototype outcomes disclose that NPRF exceeds different existing ways considerably in terms of precision, coverage and feedback range [6]. Zainab *et al.* [7] reported Content-Based Image Retrieval (CBIR) with the help of four feature extraction procedures. The four methods used are colored histogram features methods, properties options technique, grey level co-occurrence matrix (GLCM) statistical methods and hybrid methods. The options are extracted from the informative pictures and query images so as to search out the similarity measure between them. The similarity-based matching is post extraction stage in CBIR. The three sorts of similarity measure used are normalized Mahalanobis distance, Euclidean distance and Manhattan distance. The analysis concluded that CBIR using hybrid technique have higher match performance all told quite similarity measures used [7].

3 Implementation Details

3.1 System Framework of Proposed System

The aim of the methodology is to guard the safety in terms of privacy of image consumers and security for pictures each throughout storage and access against curious outsiders and to beat all issues like data integrity, data privacy, and copy deterrence, watermarking, and outsourcing the encrypted images and associated difficult problems. This framework secures the protection of picture information in substance-based picture recovery redistributing applications against an inquisitive cloud server and the exploitative question clients. Distributed computing offers an incredible open door for the on-request access to abundant calculation and capacity assets, which settles on it an appealing decision for the picture stockpiling and CBIR redistributing. The hashing algorithm is used only for auditing and indexing of the image. In auditing fraud detection and editing is being held or not is checked. The encryption algorithm is only used to cipher plain text into encrypted text. On another side, if encrypted is being tried to edit or make deletion changes in the ciphertext, after decryption the text will be incomplete or rather incorrect and the message couldn't be understood, for that case hashing algorithm will work by detecting fraud and making us alert.

Watermark and encryption are used for multimedia files together. If we encrypt multimedia data or files, then it may get corrupt or damaged. Data is encrypted first and then we embed an image with the help of watermark, so that text hidden in the image will not be damaged. Mostly encrypted image or multimedia file is clearly got to know that it is secured or private data, so as to misguide hacker or intruders by illusion image is not secured or not encrypted or no hidden text or message is embedded. Watermark cannot be edited or deleted. If that multimedia file is misplaced or used by any other employee of the company, then watermark will work as like filter or firewall, so that important files which are watermark with company logo those files only will be accepted by system, and important files which are not having company logo as watermark on documents or file those files will be rejected, as it will provide double security. We are

encrypting watermark embedded on file. Following are the phases which describe how the proposed system works gradually:

- Original images are encrypted by image owner on cloud server, meanwhile encrypted index of those images are saved on the cloudserveralong with user authentication information.
- A watermark-based protocol is applied to those images.
- Image owner sends the suspicious image to Watermark Certification Authority (WCA) checks for the possible illegal distributor. User lists are stored with WCA by image owner.
- WCA generates a watermark on those secured images and transfers them towards cloud server.
- After that encrypted images are embedded with a watermark on a cloud server.
- Once the watermark is embedded then the search image result is forwarded to image users. Image user now will fire image query and features will be extracted.
- CBIR will check similarity measures between fired image query and stored database of images.
- The image is processed by indexing and image retrieval scheme with the help of CBIR.
- Then the human interaction system i.e. Relevance Feedback System will give the result as relevant or irrelevant images iteratively with the help of users preferences.
- After that user will give proper feedback for the retrieved result, if yes then the final refined result will be displayed and if not, then again the system will check similarities matching measure and will again ask for relevance feedback iteratively.
- Final refined results will be images with a watermark, otherwise alert generation is sent back to the image owner.
- Images are decrypted and the watermark will be extracted back again as per user's requirement.

System components, the constituents of a system include Feature Extraction, Index Generation, Watermark Embedding, Image Encryption, Trapdoor Generation, Cloud Upload, Cloud Received, and Relevance Feedback. In Feature Extraction an image is processed and extracted to obtain RGB values from the color of images. With the help of hashing and signature, index and the secret key is generated in the Index generation process. The proposed system's flow chart is described in figure 1.

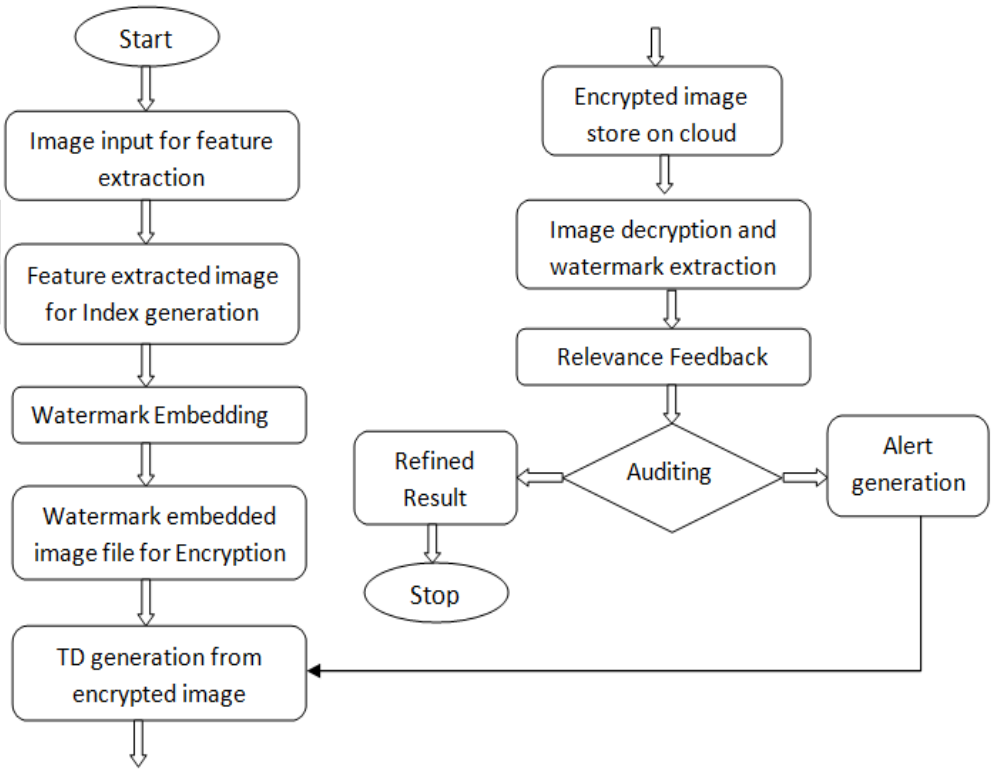

Figure 1: *Flow chart for the proposed system*

- Feature Extraction: An image is processed and extracted to obtain RGB values from the color of images.
- Index Generation: With the help of hashing and signature, index and the secret key is generated.
- Watermark Embedding: Watermark is embedded in the image.
- Image Encryption: For encrypted image format, Encryption algorithm i.e. AES encryption is used.
- Trapdoor Generation: Trapdoor i.e. secret key which is generated at the time of index generation is generated.
- Cloud Upload: A file is uploaded on a cloud server
- Cloud Retrieved: Decrypted image format with no fraud and watermark is extracted, using the Decryption algorithm i.e. AES decryption, as well as watermark extraction algorithm.
- Relevance Feedback: Match result is displayed, i.e. relevant image result is displayed, using a Bayesian network algorithm for relevant image adoption.

The planned system consists of a sequence of algorithms that are performed by completely different entities. Given a picture group *M*, the image owner builds KeyGen, IndexGen, and ImgEnc to get the set of secret keys *K*, the secure index *I*, and therefore the encrypted picture collection *C*, severally. From that time forward, the picture proprietor re-appropriates the list *I* and the buildup *C* to the cloud server, and at the moment send the key set *K* to the approved image consumers. Furthermore, the picture proprietor sends the arrangement of client personalities {*UIDi*} to watermark certificate authority (WCA). In the wake of accepting {*UIDi*}, WCA creates a special watermark *wi* for each inquiry consumer by WatermarkGen, and at the moment sends the arrangement of watermarks {*wi*} to the cloud server [1]. As explained in paper [1] following are the pseudo codes used in the proposed system.

Image Owner Side:

- $K \leftarrow$ KeyGen (1^k), is the key generation algorithmic rule that takes the safety parameter *K* as input and returns the set of secret key *K*.
- $I \leftarrow$ IndexGen (*K, M*) is the index generation algorithmic rule that takes the set of secret key *K* and also the image collection *M* as input and returns the index *I*.
- $C \leftarrow$ ImgEnc (*K, M*) is the image secret writing algorithmic rule that takes the set of secret key *K* and collection of images *M* as input and returns the encrypted collection of image *C*.

Image Consumer Side:

- $TD \leftarrow$ TrapdoorGen (K, m_q) is the trapdoor generation algorithmic rule that takes a set of key *K* and query image m_q as input and query trapdoor *TD* is returned.
- $M_q \leftarrow$ ImgDec (K, R') is the cryptography algorithmic rule that takes secret key set *K*, retrieved set of encrypted and watermarked pictures R' as input and set of watermarked images M_q is returned.

Cloud Server Side:

- $R \leftarrow$ Search (*I, C, TD*) is the search algorithm that takes encrypted collection *C*, index *I*, and trapdoor *TD* as input and the temporary search result set *R* is returned.
- $R' \leftarrow$ WatermarkEmb (R, w) is the watermark embedding algorithmic rule that takes the temporary search result set *R* as well as watermark *w*, as input and returns the set of watermarked pictures R'.

WCA Side:

- $\{W_i\} \leftarrow$ WatermarkedEn ($\{UID_i\}$) is the watermark generation algorithmic rule that generates a novel watermark W_i for every UID_i.
- $W_t \leftarrow$ WatermarkExtra (m_t, m_o) is the watermark extraction algorithmic rule that takes indistinct image m_t, as well as its original version m_o as input and the extracted watermark W_t, which is employed for the intervention is returned.

So as to recover comparable pictures, the approved picture client runs TrapdoorGen to provide an issue trapdoor *TD* and then presents the trapdoor *TD*, *UID*, and validation key to the cloud server. When accepted the pursuit provoke, the cloud server right off the flap confirms the identity of the consumer with

the *UID* and also with a secret key. Within the event that effectively confirmed, the cloud server runs a probe to acquire a short outcome set *R* as well as the most effective *k* most comparative photos. Next, the cloud server finds the watermark w following with client's *UID* and installs the watermark w into each one of the photographs in *R* by WatermarkEmb [1]. Ultimately, the watermarked image set R' is generated and sent to the querying user. When receiving R', the querying user builds ImgDec to get the set of decrypted pictures M_q. Considering that the decrypted pictures can still contain the watermark in them. Image owner will simply acquire his image group from the cloud server. WCA then extracts watermark w_t from m_t through WatermarkExtra and identifies the potential misappropriated querying user whose associated watermark is analogous to the extracted watermark w_t [1].

3.2 Flowcharts

3.2.1 Auditing

Protection checks at the cloud are essential in light of the reality that computes sharing facts are most right away available to an invader. Without mechanisms in the vicinity to detect attacks as they occur, a system might not recognize its security. Consequently, it's far vitally crucial that computers residing in the cloud are cautiously monitored for a huge variety of audit activities. The auditing in a machine consists of 3 steps. The first step is the attack has tried on any node inside the system; secondly, the assault is detected by way of the system of hashing algorithm after detection of attack the notifications are dispatched to the facts proprietor. Due to this safety is progressed. As described in flowchart for auditing, hashing and alert generation is as described below in figure 2 [8].

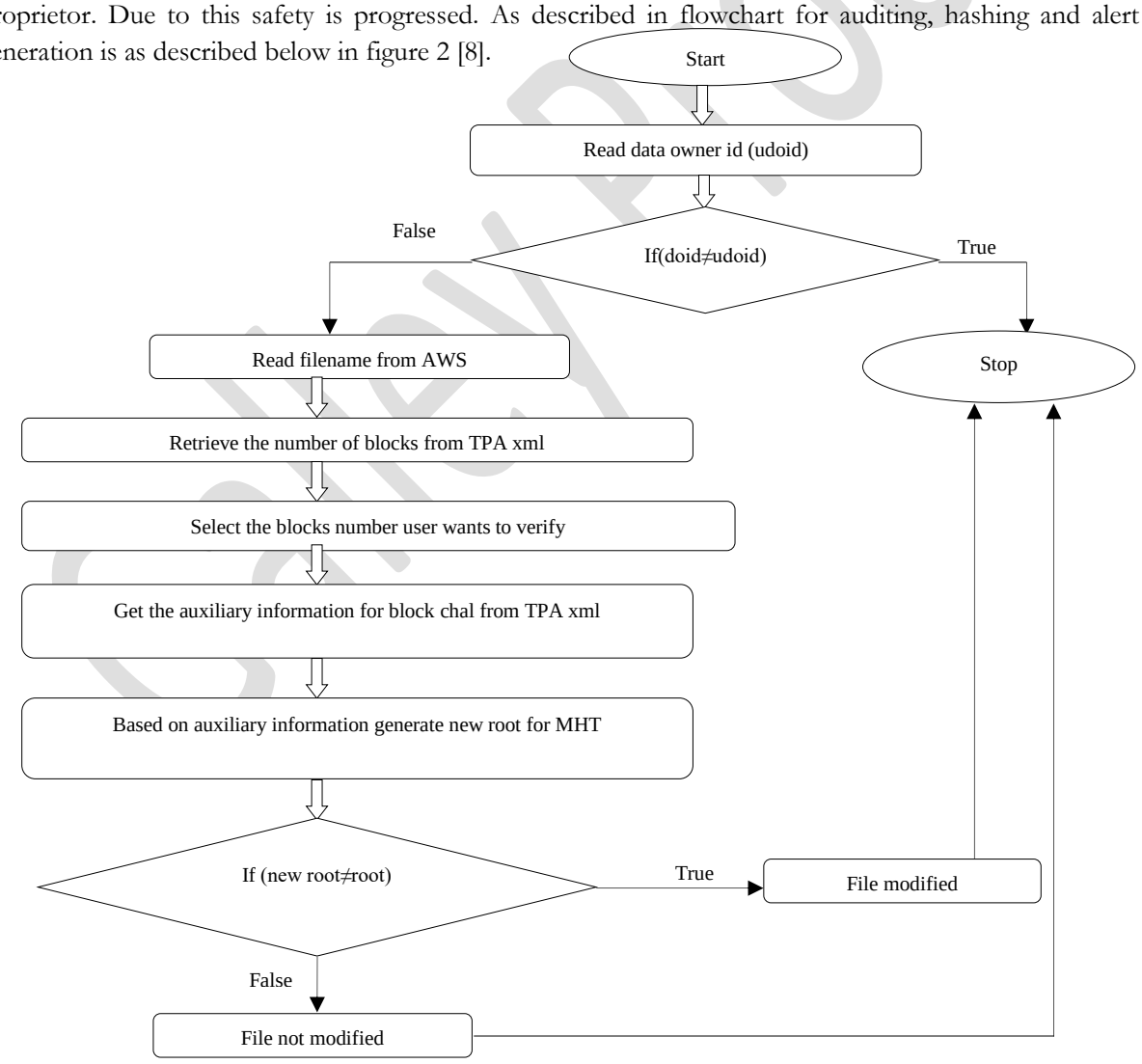

Figure 2: *Flowchart for Auditing Pseudo code*

3.2.2 Relevance Feedback

Relevance feedback system will increase the accuracy of output and will deliver the most relevant output. For increasing the accuracy rate of output and for delivering the most relevant output relevance feedback system is being used. Multiple layer feedback system over encrypted images are a unique contribution. Pseudo code for Relevance Feedback using Bayesian Network described below is referred from the paper [9] and shown in Figure 3.

1. After the initial feedback, all the relevant images are used to build the Bayesian Network.
2. Perform the updating operation of all nodes.
3. Select relevant images of positive feedback data
4. Update link weights
5. Set updated belief values as new prior beliefs for the next iteration
6. Using updated positive feedback new iteration is started
7. IF the user continues to give feedback judgment
   a. New relevant objects get added to the network
   b. Go back to step 2 with the updated weights and prior beliefs
8. Else stop the retrieval process and wait for the new query.

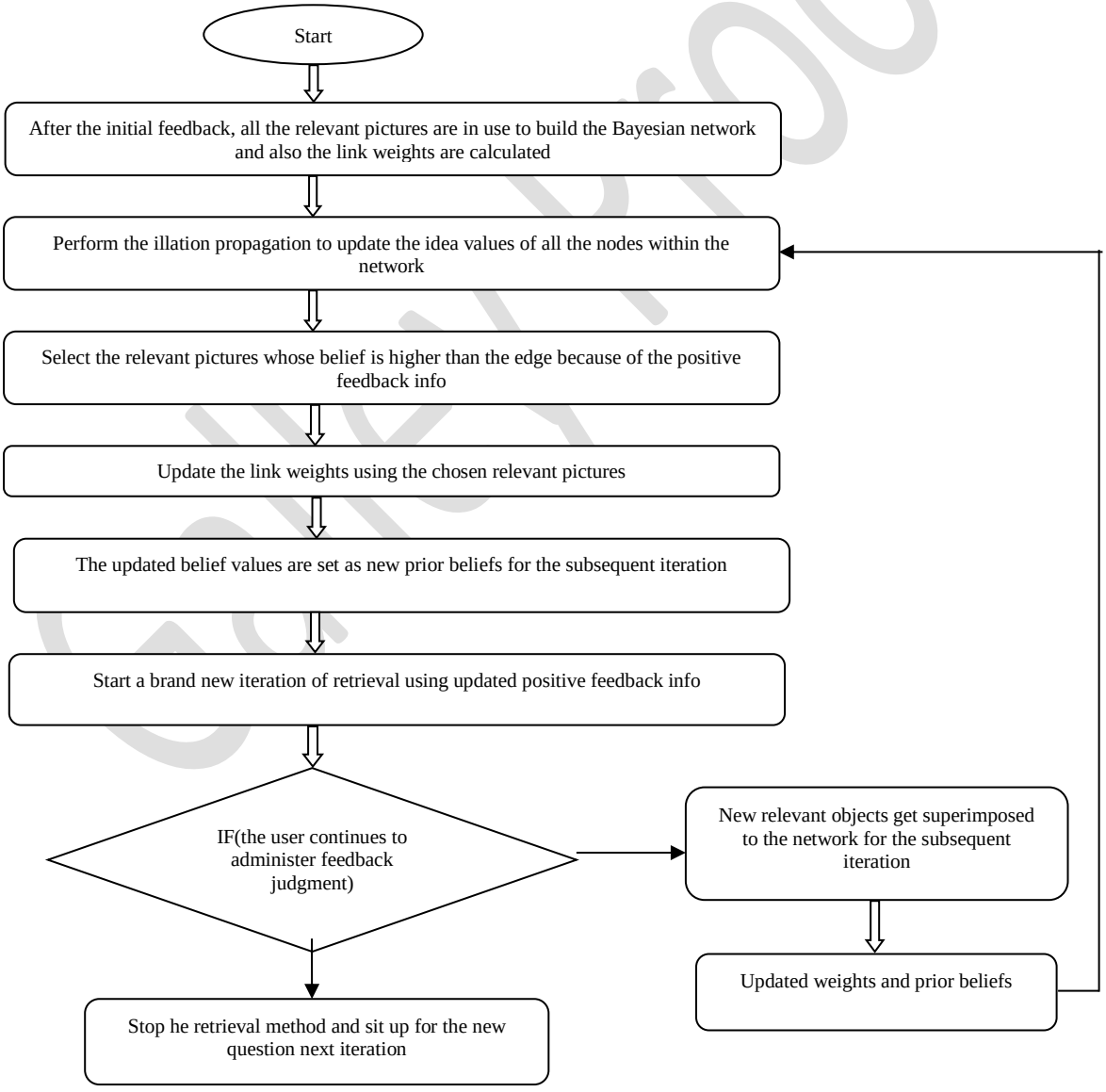

Figure 3: *Flowchart for Relevance Feedback*

4 Experimental Results

4.1 Time Consumption of Index Generation

Prior to index construction, we have completed the feature extraction. Therefore, the time consumption of index construction in our demonstration primarily includes two elements as it is described in the paper [1]:

I. The utilization of building *L* hash tables,
II. The utilization for encrypting the feature vector with a rending operation and two increasing operations with *(l+1) * (l+1)* matrices.

So as to construct a pre-filter table, it takes *O(nλl)* time to come up with the bucket values, wherever *n* denotes the entire variety of pictures, *l* denotes the spatial property of the feature vector, and λ denotes the number of articulated hash functions. The time quality of the splitting operation is *O(nl)*, and therefore the time quality of the matrix operation is *O(nl2)*. In total, the time qualifying for the index construction is *O(Lnλl + nl + nl2)*. Since *L, λ, and l* are fastened constants in our theme, the time consumption of the index construction is nearly linear to the scale of image construction, i.e., *O(n)*. Figure 4 shows the graph regarding time potency of index generation. It has been shown by the simulator that describes what quantity time the index generation module needs, it offers details of your time needed is in milliseconds. Here it has taken solely 10 milliseconds.

4.2 Time Utilization of Watermark Embedding

The planned watermark algorithmic program embeds watermark bits by flipping image pixels in line with every bit flipping proportion [ϵ_1, ϵ_2, …., ϵ_8].

The number of the flipped bits equals to [1],

$$\sum_{i=1}^{8} \varepsilon_i \times N_\omega \times S^2/2.$$

The time quality of flipping is,

$$O(N_\omega \times s^2).$$

Figure 4 gives information about the graph of time efficiency of watermark embedding. It gives details of the time required for embedding a watermark in an image. Here it has taken 230 milliseconds to embed an image. This is also shown with the help of a simulator

4.3 Time Consumption of Trapdoor Generation

Figure 4 shows how much time is consumed by the trapdoor generation component. Similar to the index generation, the trapdoor generation incurs the calculations of bucket values, a splitting operation, and two matrix multiplications as described in the paper [1]. The time complexness is *O(Lλl + l = l2)*. The time value of the trapdoor generation is principally smitten by the spatial property of the visual descriptor. Here trapdoor generation component has taken 150 milliseconds time to generate a TD.

4.4 Time Consumption of Relevance Feedback

Figure 4 shows how much relevance feedback component has taken time for searching for a relevant image. It has taken 12 milliseconds to give a relevant image as output. We have generated a small module which is built in C# and .net. It shows the time difference taken by the two algorithms DES and AES converting plain text into an encrypted form. We have calculated the time taken by each algorithm in milliseconds of encrypted data. In the proposed system, the AES algorithm is used while in existing system DES algorithm is used. Here in the above chart as shown in figure 5, the proposed system has taken only 1.2 milliseconds of time to encrypt while DES i.e. existing system took 8 milliseconds for the encryption process. This proves that AES is a better algorithm to use for the encryption process.

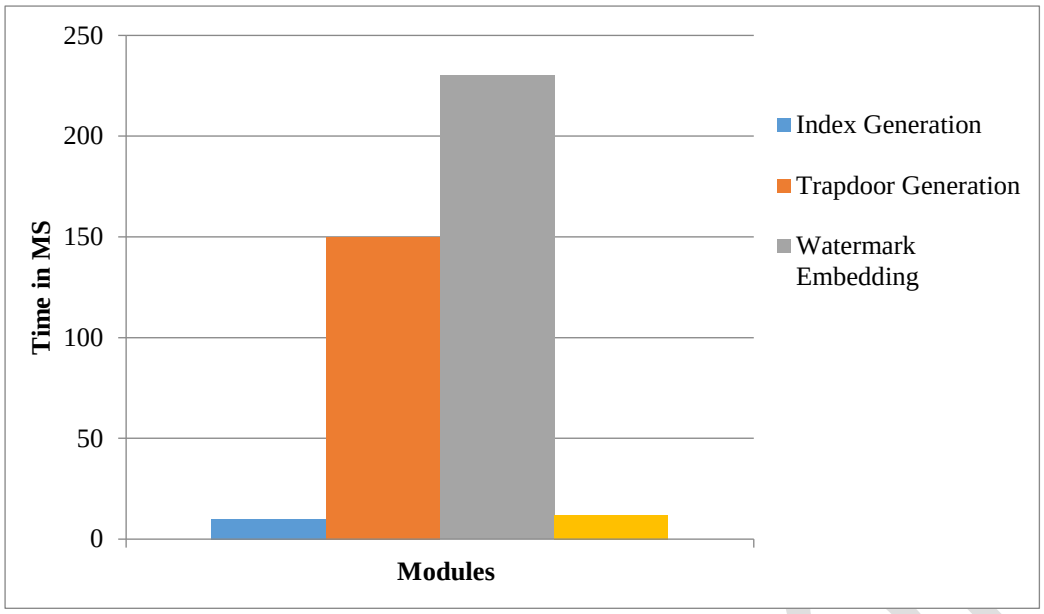

Figure 4: *Time Consumption of Index Generation, Trapdoor Generation, Watermark Embedding and Relevance Feedback*

4.5 Time comparison between Existing and Proposed system

Figure 5 shows how much time was taken by the existing and proposed system.

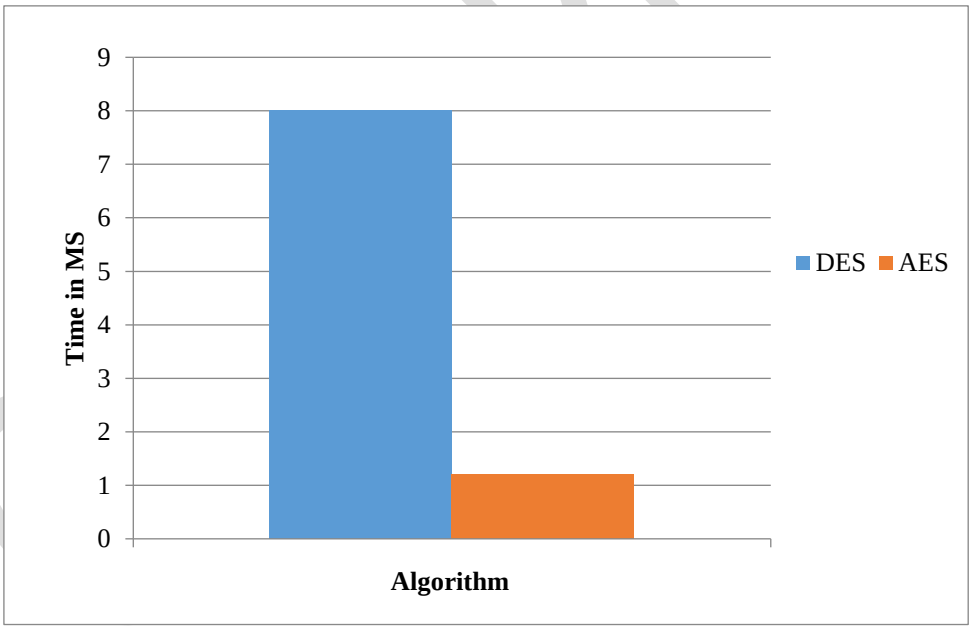

Figure 5: *Time comparison between Existing and Proposed System*

5 Conclusion

The certainty of pictures is well-kept by coding with the assistance of AES counts. The usage of content-based image retrieval gets the prospect to plot updates consumer assurance. Inquiry capability is practiced as the record is made using a Locality-Sensitive Hashing technique. We consider dishonest clients in open encryption plots and planned a watermark-based tradition for selecting the unlawful course of pictures. By and enormous, the photographs and their substance are secure against cryptography ambushes. The protection of images, clients, and copyright for footage are exceptionally practiced. Also, essential responsibility or spotlight was on the difficulty of upgrading the ampleness in making use of the relevant

pictures stated by the client's input. We proposed a strategy employing a Bayesian system because the necessary image choice show is an immeasurable resource that is proper in the point of view of pertinence criticism in picture recovery. To handle the issue of imbalanced dataset causes corruption in the recovery results, a long-haul learning approach dependent on arbitrary timberland classifier is proposed. The long-haul learning importance input gathers the client criticism, to prepare the arbitrary woodland classifier, for improving the recovery results.

6 Acknowledgments

I am truly grateful and feel blessed that I got Asst. Prof. Ms. S. Y. Gaikwad as a mentor, who has guided me always in every phase of my research work. I would also like to thank my college MPGI, for their valuable support and encouragement.

7 How to Cite this Article:

References

[1] Zhihua Xia, Xinhui Wang, Liangao Zhang Qin, Xingming Sun, and Kui Ren, "A privacy-preserving and copy-deterrence content-based image retrieval scheme in cloud computing", in *IEEE Transactions on Information Forensics and Security*, vol. 11, Issue: 11, pp. 2594-2608, Nov. 2016.

[2] K. Belattar and S. Mostefai, "CBIR using relevance feedback: comparative analysis and major challenges", IEEE 2013 5th International Conference on Computer Science and Information Technology, pp. 317-325, 27-28th March 2013.

[3] Aarti Datir, Dipak Patil "Survey on different techniques of CBIR", in *International Journal of Science Technology Management and Research (IJSTMR)*, vol. 1 Issue 8, pp. 29-34, Nov 2016.

[4] Sakshi Shivhare, Vijay Trivedi and Vineet Richhariya, "Content-based image retrieval by using Interactive relevance feedback technique- A survey", in *International Journal on Recent and Innovation Trends in Computing and Communication* (IJRITCC), vol. 3, Issue: 7, pp. 4641-4646, July 2015.

[5] Urvi H. Panchal, Rohit Srivastava, "A comprehensive survey on digital image watermarking techniques", in IEEE *2015 Fifth International Conference on Communication Systems and Network Techniques*, pp. 591-595, 4-6th April 2015.

[6] Ja-Hwung Su, Wei-Jyun Huang, Philip S. Yu and Vincent S. Tseng, "Efficient Relevance Feedback for Content-Based Image Retrieval by Mining User Navigation Patterns", *in IEEE Transactions On Knowledge And Data Engineering*, Vol. 23, Issue: 3, pp. 360-372, March 2011.

[7] Zainab Ibrahim Abood, Israa Jameel Muhsin, Nabeel Jameel Tawfiq, "Content-based Image Retrieval (CBIR) Using Hybrid Technique" in International Journal of Computer Applications, Vol. 83, No. 12, pp. 17-24, December 2013.

[8] Ajinkya Sabale, Rohit Prajapati, Sameer Patahn, Sanket Prabhu, Sanjay Agrawal, "Third-party auditing of data on a cloud with fine-grained updates", in *International Journal of Engineering and Computer Science*, vol. 4, Issue 11, pp. 14987-14992, Nov 2015.

[9] Jing Xin, Jesse S. Jin, "Relevance feedback for content-based image retrieval using Bayesian Network", ACM-ICPS *ACM International Conference Proceeding Series*, VIP '05 Proceedings of the Pan- Sydney area workshop on Visual information processing, Vol.36, pp. 91-94, 2003.